Advanced nominal techniques

Murdoch J. Gabbay

3rd School on Foundations of Programming and Software Systems
(FoPSS 2019, Warsaw, 10–15 September 2019)

14-15 September 2019

Thanks

It's a pleasure to be here.

Thank you to the organisers.

Quiz: who self-identifies as primarily

1. A programmer?
2. A mathematician?
3. A computer scientist?

Foundations

Andrew once commented that I was the first 'nominal native'. By this he meant that I've never known anything else.

For these lectures I'll work in Equivariant ZF set theory with Atoms and Choice (EZFAC).

We'll be native: names and permutations are furniture in our universe.

You're probably a ZFC native, and that's fine, but it is only for slightly arbitrary historical reasons.

The University of Warsaw library is a wonderful place to be able to say this.

Foundations

Because we're in EZFAC, our sets universe has powersets (as usual) building up with

- a base set of atoms (urelemente) $\mathbb{A}$ and
- an equivariance axiom-scheme

$$(\mathbf{E}) \qquad \Phi(x_1, \ldots, x_n) \Leftrightarrow \Phi(\pi \cdot x_1, \ldots, \pi \cdot x_1)$$

for every permutation π & assertion Φ on elements $x_1, \ldots, x_n$.

Foundations

Lemma: Equivariance (**E**) is consistent with Choice.
If $f : pow^*(X) \to X$ is a choice function on X, then $\pi \cdot f$ is one on $\pi \cdot X$.

Choice functions cannot in general be arrows in the Schanuel topos / Category of Nominal Sets, and cannot be elements in the universe of Fraenkel-Mostowski sets.

We would be wise to be careful not to mislead readers by translating this precise mathematical fact imprecisely to a slogan that 'nominal techniques are inconsistent with the Axiom of Choice', as Lemma above illustrates.

Foundations

Every instance of (**E**) is *derivable* in ZFA. In symbols:

$$ZFA \vDash (\mathbf{E}).$$

Thus EZFAC and ZFAC are equivalent, as are EZFA and ZFA!

However, the ZFA derivation of a Φ-instance of (**E**) scales with the complexity of Φ. The above is a meta-theorem, parameterised over the choice of Φ. This is

- fine if you're handwaving but not fine if you're not, and
- readers are typically unused to foundational meta-theorems (unless historically familiar, e.g. consistency strength or incompleteness arguments), and therefore distrustful of them.

Nominal algebra

I therefore take (**E**) as a direct axiom-scheme:

- whatever we say about elements mentioning one collection of atoms (even if that collection is infinite!)
- must by (**E**) also be true if we permutatively rename those atoms (even if the permutation is infinite!).

I think it might be helpful if we made these points more often and more explicitly. See [equzfa].

So that's our universe.

Nominal algebra

Let's start with perhaps the simplest interesting logic: algebra, the logic of equality.

What does algebra look like in a universe with atoms?

Nominal algebra has the syntax of nominal terms-in-context, and the natural semantics in sets with atoms.

Assume sets $a \in \mathbb{A}$ and $X \in \mathbb{X}$ (unknowns). Terms of Nominal Algebra:

$$s ::= a \mid \pi{\cdot}X \mid \mathsf{tf}(s, \ldots, s) \mid [a]s$$

- a is an atom.
- $\pi{\cdot}X$ is a permutation π suspended on a unknown X.
- tf is a term-former (fixed in a signature).
- $[a]s$ is atoms-abstraction. The a in $[a]s$ does not α-convert; this is handled by the equational theory.

Judgements

We can easily type term-formers and terms, but I'll use untyped/monotyped syntax for simplicity.

A freshness constraint is a pair $a\#X$ of an atom and an unknown.

A freshness context Δ is a finite set of freshness constraints.

Nominal algebra judgements have the form

$$\Delta \vdash s = t.$$

Call this an equality-in-freshness-context.

Looks very much like a rewrite-in-freshness-context $\Delta \vdash s \to t$, but what we do with equalities is different (soundness, completeness, models, duality, HSP, derivation, etc).

Example judgements

These are expressive; we abbreviate $id{\cdot}X$ to X:

$$a, b\#X \vdash (a\ b){\cdot}X = X$$
$$b\#X \vdash [b](b\ a){\cdot}X = [a]X$$
$$\vdash \mathsf{sub}([a]X, Y) = \mathsf{sub}'(X, a, Y)$$
$$a\#Y \vdash \mathsf{sub}(\mathsf{lam}([a]X), b, Y) = \mathsf{lam}([a]\mathsf{sub}(X, b, Y))$$

- α-equivalence (top two equations are the theory of α-equivalence).
- Swappings.
- Atoms-abstraction.
- Substitution.
- The λ-calculus.
- First-order logic.
- String diagrams, . . . and more to follow.

Models

Fix a nominal set $\mathfrak{M}$ and a signature and

- interpretations $[\![tf]\!]^{\mathfrak{M}} : \mathfrak{M}^n \to \mathfrak{M}$, and
- a function $[\text{-}]^{\mathfrak{M}}\text{-} : \mathbb{A} \times \mathfrak{M} \to \mathfrak{M}$ such that $a\#[a]^{\mathfrak{M}}x$ always.

A valuation ς maps unknowns to elements of $\mathfrak{M}$.

Given $\mathfrak{M}$, interpretation is:

$$[\![\pi \cdot X]\!]_\varsigma = \pi \cdot \varsigma(X)$$

$$[\![[a]s]\!]_\varsigma = [a]^{\mathfrak{M}}[\![s]\!]_\varsigma$$

$$[\![\mathrm{tf}(s_1, \ldots, s_n)]\!]_\varsigma = \mathrm{tf}^{\mathfrak{M}}([\![s_1]\!]_\varsigma, \ldots, [\![s_n]\!]_\varsigma)$$

$$[\![a\#s]\!]_\varsigma = (a\#[\![s]\!]_\varsigma)$$

$$[\![\Delta]\!]_\varsigma = \bigwedge\{a\#\varsigma(X) \mid (a\#X) \in \Delta\}$$

$$[\![\Delta \vdash s = t]\!]_\varsigma = ([\![\Delta]\!]_\varsigma \Rightarrow [\![s]\!]_\varsigma = [\![t]\!]_\varsigma)$$

Axioms

- An axiom is a judgement $\Delta \vdash s = t$.
- A theory is (a signature and) a set of axioms.

Nominal algebra has the usual properties of nominal terms equality built in, along with the following axioms:

$$a, b\#X \vdash X = (a\ b)\cdot X$$
$$b\#X \vdash [a]X = [b](b\ a)\cdot X$$

Above, X is shorthand for $id\cdot X$.

We can fix a signature and further axioms to get a theory.

Validity

A judgement is valid in a model $\mathfrak{M}$ when for every valuation ς,

$$[\Delta]_\varsigma \Rightarrow [s]_\varsigma = [t]_\varsigma.$$

The built-in axioms are valid

$$\begin{aligned} a, b\#x &\Rightarrow x = (a\ b)\cdot x \\ b\#x &\Rightarrow [a]x = [b](b\ a)\cdot x. \end{aligned}$$

Abstraction

Atoms-abstraction turns up in the semantic theory [gabbay:nomahs], so in this sense it's inherent.

Still, we do not need to make it in-built; it can be axiomatised. Assume a binary term-former abs:

$$b\#X \vdash \mathsf{abs}(a, X) = \mathsf{abs}(b, (b\ a)\cdot X)$$

Restriction is similarly axiomatisable:

$$b\#X \vdash \mathsf{res}(a, X) = \mathsf{res}(b, (b\ a)\cdot X)$$
$$a\#X \vdash \mathsf{res}(a, X) = X$$

Maribel Fernández and I studied these two side-by-side in a paper [gabbay:nomrng]. Syntax was different, not least because Nominal Algebra hadn't been invented.

Axiomatise swappings

It's surprisingly fun and useful to axiomatise swappings, even if they're in-built.

Assume a ternary term-former swap and for simplicity write $\mathrm{swap}(s, t, u)$ as $[s\ t]{\cdot}u$.

Can we spell out the theory of swappings using swap? The simplest theory would be

$$\vdash [a\ b]{\cdot}x = (a\ b){\cdot}x.$$

But this is uninformative; it's just a transation.

It's instructive to be more explicit.

Axiomatise swappings

The canonical property of swappings in nominal sets is

$$a, b\#x \Rightarrow (a\ b)\cdot x = x.$$

So is this a full theory of swappings?

$$a, b\#X \vdash [a\ b]\cdot X = X$$

Are we missing any axioms?

Yes, just a few ...

Axiomatise swappings

$$
\begin{aligned}
a, b\#X &\vdash [a\ b]\cdot X = X \\
&\vdash [a\ a]\cdot X = X \\
\\
&\vdash [a\ b]\cdot X = [b\ a]\cdot X \\
&\vdash [a\ b]\cdot[a\ b]\cdot X = X \\
&\vdash [a\ b]\cdot[c\ d]\cdot X = [c\ d]\cdot[a\ b]\cdot X \\
&\vdash [a\ b]\cdot[b\ d]\cdot X = [a\ d]\cdot[a\ b]\cdot X \\
\\
&\vdash [a\ b]\cdot[c]X = [c]\,[a\ b]\cdot X \\
&\vdash [a\ b]\cdot[b]X = [a]\,[a\ b]\cdot X \\
\\
&\vdash [a\ b]\cdot \mathrm{tf}(X_1, \ldots, X_n) = \mathrm{tf}([a\ b]\cdot X_1, \ldots, [a\ b]\cdot X_n)
\end{aligned}
$$

Above, a, b, c, d are specific atoms. In axioms, X get *instantiated*, and a, b, c, d get *permuted*.

In axioms, atoms behave like variables ranging permutatively over $\mathbb{A}$.

Axiomatise substitution

Let's do something more semantically interesting now.

Assume a binary term-former sub and sugar $\mathsf{sub}([a]t, s)$ to $s[a \mapsto t]$.

$$\vdash \mathsf{tf}(Y_1, \ldots, Y_n)[a \mapsto X] = \mathsf{tf}(Y_1[a \mapsto X], \ldots, Y_n[a \mapsto X])$$

$$b\#X \vdash ([b]Y)[a \mapsto X] = [b](Y[a \mapsto X])$$

Is this everything?

If not, what's missing?

Axiomatise substitution: the theory Sub

Assume a binary term-former sub and

$$\text{write} \quad \mathsf{sub}([a]t, s) \quad \text{as} \quad t[a{\mapsto}s].$$

Then a theory of substitution is:

$$\vdash \mathsf{tf}(Z_1, \ldots, Z_n)[a{\mapsto}X] = \mathsf{tf}(Z_1[a{\mapsto}X], \ldots, Z_n[a{\mapsto}X])$$
$$c\#X \vdash ([c]Z)[a{\mapsto}X] = [c](Z[a{\mapsto}X])$$

$$a\#Z \vdash Z[a{\mapsto}X] = Z$$
$$a\#Y \vdash Z[a{\mapsto}X][b{\mapsto}Y] = Z[b{\mapsto}Y][a{\mapsto}X[b{\mapsto}Y]]$$

$$\vdash a[a{\mapsto}X] = X$$
$$\vdash Z[a{\mapsto}a] = Z$$
$$a\#X \vdash [a]\mathsf{sub}(X, a) = X$$

Soundness & completeness provable [gabbay:capasn-jv].

Axiomatise substitution: the theory Sub

Sub is a nominal algebraic abstraction of a thing that is often called term algebras. I'd like to call a model of Sub a *nominal term algebra*.

Why are these not axioms?

$$\vdash b[a \mapsto X] = b$$

$$a' \# Z \vdash Z[a \mapsto x] = ((a'\ a) \cdot Z)[a' \mapsto X]$$

$$a' \# Z \vdash Z[a \mapsto a'] = (a'\ a) \cdot Z$$

Axiomatise substitution: the theory Sub

These axioms are derivable.

$$\begin{aligned} &\vdash b[a{\mapsto}X] = b \\ a'\#Z &\vdash Z[a{\mapsto}x] = ((a'\ a){\cdot}Z)[a'{\mapsto}X] \\ a'\#Z &\vdash Z[a{\mapsto}a'] = (a'\ a){\cdot}Z \end{aligned}$$

E.g. the third one is derived as follows:

$$\begin{aligned} a'\#Z \vdash Z[a{\mapsto}a'] &= ((a'\ a){\cdot}Z)[a'{\mapsto}a'] \\ &= (a'\ a){\cdot}Z. \end{aligned}$$

Models of Sub

Significant models of Sub include:

1. *Syntax:*
   $\mathrm{sub}([a]t, s)$ *is* $s[a{:=}t]$ [capasn-jv].
2. λ*-calculus*,
   We write $[a]t$ as $\lambda a.t$ and $t[a{\mapsto}s]$ as $(\lambda a.t)s$.
   (λ-calculus is term algebra + computational content; models differ; c.f. swapping sub axiom).
3. *Fraenkel-Mostowski sets universe*
   is a model of Sub [gabbay:stusun].
4. *Duality-based models*,
   e.g. [gabbay:semooc]. More on this later, I hope.

Nominal powersets

The nominal powerset is an interesting place. We can use nominal algebra to explore it.

Consider a nominal set $\mathbb{X}$, and its finitely-supported powerset $pow_{fs}(\mathbb{X})$.

- This is a poset via subset inclusion: $X \leq Y$ when $X \subseteq Y$.
- It's a Boolean algebra via intersection $\cap$ and complement $\mathbb{X} \setminus$ -.
- But it also has a *new-quantifier for sets*:

$$\mathsf{n}a.X = \{x \mid \mathit{M}b.x \in (b\ a)\cdot X\}.$$

This is a sets version of M: if we think of $\mathbb{X}$ as a set of points, and $X \in pow_{fs}(\mathbb{X})$ as a unary predicate on those points, then $\mathsf{n}a.X$ holds at x precisely when $(b\ a)\cdot X$ holds at x for fresh b.

Axioms of Banonas (nominal Boolean algebra with и)

Taken from [gabbay:stodnb]. Unary term-formers $\neg$ and и, binary term-former $\wedge$.

Write $\neg(s)$ as $\neg s$, $\wedge(s,t)$ as $s \wedge t$, and и$([a]s)$ as и$a.s$:

(**Commute**)		$X \wedge Y = Y \wedge X$
(**Assoc**)		$(X \wedge Y) \wedge Z = X \wedge (Y \wedge Z)$
(**Huntington**)		$X = \neg(\neg X \wedge \neg Y) \wedge \neg(\neg X \wedge Y)$
(**Swap**)		и$a.$и$b.X =$ и$b.$и$a.X$
(**Garbage**)	$a\#X \vdash$	и$a.X = X$
(**Distrib**)		и$a.(X \wedge Y) =$ (и$a.X$) $\wedge$ (и$a.Y$)
(**SelfDual**)		$\neg$и$a.X =$ и$a.\neg X$

First three axioms are a compact axiomatisation of Boolean algebra.

Last four axiomatise n$a.X = \{x \in X \mid И b.x \in (b\ a)\cdot X\}$.

(Why no axiom $b\#X \vdash$ и$a.X =$ и$b.(b\ a)\cdot X$?)

Axioms of Banonas

Are these axioms sound?

In what sense are they complete and natural?

Recall: Prime filters

If $\mathbb{B}$ is a Boolean algebra then a prime filter on $\mathbb{B}$ is a subset $p \subseteq \mathbb{B}$ such that:

1. $x \wedge y \in p$ if and only if $x \in p \wedge y \in p$.
2. $x \in p$ if and only if $\neg x \notin p$.

Recall: Stone representation for Boolean algebra

- Take a Boolean algebra $\mathbb{B}$.
- Write $\mathit{points}(\mathbb{B})$ for the prime filters over $\mathbb{B}$.
- For $x \in \mathbb{B}$, define

$$x^\bullet = \{p \in \mathit{points}(\mathbb{B}) \mid x \in p\} \in \mathit{pow}^2_{fs}(\mathbb{B})$$

$$\mathbb{B}^\bullet = \{x^\bullet \mid x \in \mathbb{B}\} \qquad \subseteq \mathit{pow}^2_{fs}(\mathbb{B})$$

Theorem: $x \longmapsto x^\bullet$ bijects $\mathbb{B}$ with $\mathbb{B}^\bullet$.

By prime filter conditions, $-^\bullet$ converts conjunction $\wedge$ into intersection $\cap$, negation $\neg$ into sets complement $\mathbb{B}^\bullet \setminus -$. Thus:

- Any powerset is naturally a Boolean algebra.
- Any Boolean algebra is (isomorphic to) a Boolean algebra over set; recipe above.

Representing Banonas

How does the picture look for Boolean algebras with И? These are the Banonas of [stodnb].

The Banona axioms are sound for intersection, complement, and n — but do we get an *isomorphism*?

What are correct notions of prime filter and -$^\bullet$ that bijект Banonas with a powersets model?

By definition $x^\bullet = \{p \in \mathit{points}(\mathbb{B}) \mid x \in p\}$.

We expect lemmas that:

- $(x \wedge y)^\bullet = x^\bullet \cap y^\bullet$, and
- $(\neg x)^\bullet = B^\bullet \setminus x^\bullet$, and
- $(\text{И}a.x)^\bullet = \text{n}a.(x^\bullet)$
  $= \{p \in \mathit{points}(\mathbb{B}) \mid \text{И}b.p \in (b\ a)\cdot(x^\bullet)\}$
  $= \{p \in \mathit{points}(\mathbb{B}) \mid \text{И}b.p \in ((b\ a)\cdot x)^\bullet\}$ *How this?*
  $= \{p \in \mathit{points}(\mathbb{B}) \mid \text{И}b.(b\ a)\cdot x \in p\}$.

Representing Banonas

Let $\mathbb{B}$ be a Banona.

A prime filter on $\mathbb{B}$ is a *finitely-supported* subset $p \subseteq \mathbb{B}$ such that:

1. $x \wedge y \in p$ if and only if $x \in p \wedge y \in p$.
2. $x \in p$ if and only if $\neg x \notin p$.
3. If $a\#p$ then $x \in p$ if and only if $и a.x \in p$.

With these definitions, $\mathbb{B}$ bijects with $\mathbb{B}^\bullet$.

In $\mathbb{B}^\bullet$, condition 3 above translates to "if $a\#X$ then $p \in X$ if and only if $p \in \mathrm{n}a.X$".

So our axioms for $и$ are correct in the sense that any Banona can be represented as a Banona over sets, in which $и$ corresponds precisely to the $И$-quantifier on nominal sets.

Representing Banonas

The paper [stodnb] contains more complexity than this.

- The proofs are quite subtle.
  Critical point: how to expand a filter to a maximal filter, while retaining finite support.
  Critical point: a filter $p \subseteq \mathbb{B}$ is maximal amongst p' such that $\mathrm{supp}(p') \subseteq \mathrm{supp}(p)$, if and only if p is maximal amongst all p'.
- There's a complete treatment of topologies and duality.

First-order logic

Assume $\mathbb{X}$ is a model of Sub, so $\mathbb{X}$ is an abstract notion of term-algebra.

What structure does $pow(\mathbb{X})$ inherit from Sub?

(This material comes from [stodfo].)

We get an amgis-algebra (dual of sigma-algebra).

Assume a ternary term-former amgis and write amgis(u, s, a) as $u[s \leftarrow\!\shortmid a]$. Then axioms are:

$$Z[a \leftarrow\!\shortmid a] = Z$$
$$a\#v \vdash \quad Z[Y \leftarrow\!\shortmid b][X \leftarrow\!\shortmid a] = Z[X[b \mapsto Y] \leftarrow\!\shortmid a][Y \leftarrow\!\shortmid b]$$

First-order logic

Axioms are:

$$\begin{array}{rc} & Z[a{\leftarrow\!\shortmid}a] = Z \\ a\#v \vdash & Z[Y{\leftarrow\!\shortmid}b][X{\leftarrow\!\shortmid}a] = Z[X[b{\shortmid\!\rightarrow}Y]{\leftarrow\!\shortmid}a][Y{\leftarrow\!\shortmid}b] \end{array}$$

These axioms are coming from a duality property that

$$u[a{\shortmid\!\rightarrow}x] \in p \Leftrightarrow u \in p[x{\leftarrow\!\shortmid}a].$$

But note that a is abstracted on the left in $u[a{\shortmid\!\rightarrow}x]$, but free on the right in $p[x{\leftarrow\!\shortmid}a]$.

Also, a point is a maximal theory, and maximal theories in first-order logic tend to contain infinitely many choices (because they have a term language; you may be forced to complete a theory with infinitely many arbitrary choices, one for each possible value a term can take).

So we shouldn't expect p to have finite support. It won't, in general.

First-order logic

Now let's look at $pow_{fs}(pow(\mathbb{X}))$. This is a Boolean algebra, because it's a powerset.

It inherits a σ-action from the underlying $\mathfrak{o}$-action on $pow(\mathbb{X})$.

How?? If $P \in pow_{fs}(pow(\mathbb{X}))$ and $x \in \mathbb{X}$ then

$$p \in P[a \mapsto x] \Leftrightarrow \mathit{M}a'.p[x \leftarrow\!\shortmid a'] \in (a'\ a)\cdot P.$$

This builds in α-equivalence, and we recover the full Sub axioms at the level of $pow_{fs}(pow(\mathbb{X}))$.

- Sub on $\mathbb{X}$ becomes
- Amgis on $pow(\mathbb{X})$ becomes
- Sub on $pow_{fs}(pow(\mathbb{X}))$.

First-order logic

Now how do we model universal quantification in $pow_{fs}(pow(\mathbb{X}))$?

Given $P \in pow_{fs}(pow(\mathbb{X}))$, we can form:

$$\bigcup\{P' \subseteq P \mid a\#P'\}$$

$$\bigcup\{P' \subseteq P \mid \mathrm{supp}(P') \subseteq \mathrm{supp}(P) \setminus \{a\}\}$$

$$\bigcap\{\pi{\cdot}P \mid \pi \in fix(\mathrm{supp}(P) \setminus \{a\})$$

$$\bigcap\{P[a{\mapsto}x] \mid x \in \mathbb{X}\}$$

Theorem:

1. These are all equal; write the result $\forall a.P$.
2. Furthermore, $(\forall a.P)[b{\mapsto}y] = \forall a.(P[b{\mapsto}y])$.

Proof: Many calculations. See [stodfo] and [semooc].

Conclusions

Starting from nominal sets we can build a nominal algebra in a natural way.

It's compatible with nominal rewriting and in this sense there is a path from computation to logic and back.

By analysing nominal powersets we can recover the foundations of (nominal) logic, including the $И$-quantifier and first-order logic.

We create new theories of substitution (and its dual) along the way.

Representation and duality theorems can also be proved.

Just from looking at nominal powersets in EZFAC we get an account of basic mathematical foundations entirely parallel to the one developed (much of it here) based on ZFAC.